Volume 16, Issue 05   Atari Online News, Etc.   January 31, 2014

=~=~=~=

A-ONE #1605   01/31/14

   ~ Spy Agencies Tap Data! ~ People Are Talking!   ~ Yahoo Mail Hacked!
   ~ FCC Begins "Experiment" ~ Nintendo in Tough Spot ~ PS4 vs Xbox One!
   ~ Ouya Releases New Model ~ Facebook's and Privacy ~ HP Returns to Win 7!

~ People Hate Live Tiles! ~ Nadella To Be New CEO? ~ Web Votes Baby Name!

-* Borrow Your Neighbor's WiFi? *-
-* Hackers Transform Angry Birds Site! *-
-* Victim of Epic Hack Points Finger at PayPal *-

=~=~=~=

->From the Editor's Keyboard   "Saying it like it is!"
  """"""""""""""""""""""""""""

Well, the weather has "calmed" lately, at least here in the Northeast.
I feel sorry for those down South who aren't really prepared for wintry
weather. It's difficult to prepare for something which you have very
little experience. Cold temps are one thing, but snow and freezing
rain are some things to reckon with!

Here, the temps will get to around "normal" for this area over the
upcoming week. I hope it happens quickly; heating oil prices around
here aren't cheap!

Super Bowl weekend! While our local team (the Pats) got knocked out of
contention, I'll probably still watch the big game. And, it's also
about the commercials! I don't have a "favorite" in this one, but I'm
leaning a little bit toward the Broncos. Hope it's a great game!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Nintendo Is Stuck Between The Past and The Fu
ture!
  """"""""""""""""""""""""""""""   Ouya Releases New 16GB Model!
                                    Nintendo May Institute A New Discount Rewards
 Program

                                    And much more!

=~=~=~=

->A-ONE's Game Console Industry News   - The Latest Gaming News!
  """"""""""""""""""""""""""""""""""""

     Nintendo Is Stuck Between The Past and The Future of Gaming

Nintendo, which posted a 30 percent drop in profits, is undeniably in a tough spot right now.

How tough, exactly? According to the Associated Press, company president Satoru Iwata has said he ll take a 50 percent pay cut as a way of taking responsibility for falling sales of Nintendo products, including the Wii U console and hand-held Nintendo 3DS.

Legendary game creator Shigeru Miyamoto and another high-ranking director will also take a pay cut 30 percent and seven board members will cut their paychecks by one-fifth, the report said.

The actions of the board members and executives may be surprising, but the losses themselves are not. Nintendo had already indicated it was disappointed with its sales earlier this month when it drastically slashed its sales outlook for the Wii U, Wii and 3DS. The company, which has put a heavy emphasis on promoting family-friendly games, has not only had to compete with console makers Sony and Microsoft but also smartphone and tablet makers such as Apple and Samsung, which have taken over much of the gaming market. Or, put another way, Nintendo is stuck between the gaming past and the gaming future.

There are more gamers than ever today according to the Entertainment Software Association: The number of regular gamers in the world broke the 1 billion mark for the first time in 2013. It just happens that a lot of those gamers are picking up smartphones and tablets to play games instead of controllers.

Sony and Microsoft have figured out a way to keep the really hard-core gamers on consoles: Both companies sold more units of their new consoles in two weeks than Nintendo did all quarter. But, despite plunging profits, Iwata has eschewed moving Nintendo games onto the next big platform going as far as to say that the firm isn t interested in putting its games on smartphones at all.

In a statement to Engadget, the company said that there are no plans to Nintendo software on smartphones, although it is open to looking for ways to better promote its games on mobile gadgets.

In a way, it s easy to understand where Nintendo stands.

Hardware is an integral part of the company   look no further than the GameBoy. And while the Wii U, launched in 2012, has certainly failed to gain the foothold the firm needs, it s the only real console flop that Nintendo s ever had. The Wii, in fact, broke records at its launch as the fastest-selling console in history. Even previous consoles, such as the GameCube, may not have beaten Sony and Microsoft in the market, they did make money.

What may actually be most troubling out of Nintendo s earnings, then, is that sales of it s market-leading 3DS, which has helped Nintendo weather Wii U losses, are also softening. Without that cushion, Nintendo will likely have to move fast to either come up with another hit like the Wii or take a hard look at what its future should be.

Nintendo May Institute A New Discount Rewards Program

Along with the many other announcements coming out of Satoru Iwata in recent days regarding how Nintendo can turn their fortunes around, it appears that Nintendo might be adding more incentives for those who are loyal to the brand. They already have Club Nintendo, a place where you can register your purchases and earn points towards trinkets and occasionally get exclusive access to downloadable games, but now they are fishing around something more substantial.

The plan is to discount future purchases for those who buy tons of games and refer their friends and family as well. While selling consoles is a key part of the gaming business, software sales are where the real dough is made and Nintendo hopes to galvanize those software sales while they attempt to bring the Wii U up in the rankings. Nintendo has always had the market cornered on price point, and this could give them even more of an advantage in the budget gaming area and might just give them the boost they need.

This is noteworthy for another reason. The only way to track these purchases would be through a unified account system, something that Iwata mentioned in the brief and what consumers have been calling for in droves. The Nintendo Network ID will work across the Wii U and 3DS, and hopefully it ll integrate some of the social networking functionality found on PSN and Xbox Live.

For Nintendo s sake let s hope it isn t too little too late.

PS4 vs Xbox One News, Games, and Comparison:
Microsoft Tries to Take Back Console War By Buying Old PlayStations

In terms of sales, Microsoft's Xbox One is losing to Sony's PlayStation 4 in the console war, but just barely. Now, Microsoft has thought of a way to outshine another unlikely competitor: gamers' old PlayStation 3 systems.

Microsoft announced that it will give gamers $100 worth of store credit in exchange for old systems. The company made sure to name the PS3 explicitly. The Xbox 360 S and Xbox 360 E can also be traded in to get the $100 credit. Customers do not necessarily have to use the credit toward a new Xbox One, but it is obvious that Microsoft hopes that gamers will decide to do so.

"Trade up and get your hands on the new Xbox One," the offer page reads. "Welcome to a new generation of games and entertainment. Where games push the boundaries of realism. And television obeys your every command. Where listening to music while playing a game is a snap. And you can jump from TV to movies to music to a game in an instant. Where your experience is custom tailored to you. And the entertainment you love is all in one place."

The deal is available until Mar. 2.

Ouya Releases New 16GB Model

Ouya s Android-console revolution now has extra space for games.

The company is now selling a 16GB version of its microconsole for $130.
This means that gamers can now download and store more games. The system
is available for purchase right now from Ouya s official website.

In addition to the extra storage space, the new system features an all
matte-black finish. The hardware designers also boosted the console s
Wi-Fi capabilities, which will help it stay connected even when it is
sitting far away from a wireless router.

Finally, the 16GB model comes with a refined controller that also has a
matte-black finish that features better analog sticks and face buttons.

Ouya will continue selling the original 8GB console for $100.

The Ouya system is a tiny console that runs a variation on Google s
Android OS. The idea behind the system is to bring simple, mobile-style
distribution to televisions.

Ouya (the company, not the console) first introduced the product during a
Kickstarter in 2012 that ended up raising more than $8.5 million. The
consumer release went on sale in June.

                              =~=~=~=

->A-ONE Gaming Online   -   Online Users Growl & Purr!
   """"""""""""""""""""

        Rare Nintendo World Championships Cart Fetching $5K on eBay

Nintendo fans and game collectors, listen up: an exceedingly rare game is
available right now on eBay.

An eBay user recently posted Nintendo World Championships on the auction
site. The cartridge, if real as the seller claims, is one of only 116
copies created, making it one of the most exclusive titles ever made for
the Nintendo Entertainment System.

Nintendo World Championships was part of a special event the company held
in 1990 for gamers to compete in Super Mario, Rad Racer, and Tetris. The
game was never actually sold to consumers on store shelves.

As of this writing, Nintendo World Championships is bidding out at $5,500
with another day to go. The cartridge is in somewhat poor state, but the
owner says it's still in working condition.

According to the BBC, which earlier reported on the auction, a copy in
better condition sold at a charity auction in 2011 for $11,000.

                              =~=~=~=

Spy Agencies Tap Data Streaming From Phone Apps

When a smartphone user opens Angry Birds, the popular game application, and starts slinging birds at chortling green pigs, spies could be lurking in the background to snatch data revealing the player s location, age, sex and other personal information, according to secret British intelligence documents.

In their globe-spanning surveillance for terrorism suspects and other targets, the National Security Agency and its British counterpart have been trying to exploit a basic byproduct of modern telecommunications: With each new generation of mobile phone technology, ever greater amounts of personal data pour onto networks where spies can pick it up.

According to dozens of previously undisclosed classified documents, among the most valuable of those unintended intelligence tools are so-called leaky apps that spew everything from the smartphone identification codes of users to where they have been that day.

Today's smartphones are nothing more than nicely packaged tracking devices that the user proudly and naively brings wherever they go.

The N.S.A. and Britain s Government Communications Headquarters were working together on how to collect and store data from dozens of smartphone apps by 2007, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor. Since then, the agencies have traded recipes for grabbing location and planning data when a target uses Google Maps, and for vacuuming up address books, buddy lists, telephone logs and the geographic data embedded in photographs when someone sends a post to the mobile versions of Facebook, Flickr, LinkedIn, Twitter and other Internet services.

This document from 2010, redacted in places, is one of several undisclosed classified documents provided by Edward J. Snowden, the former N.S.A. contractor, and shared by The New York Times, The Guardian and ProPublica.

The eavesdroppers pursuit of mobile networks has been outlined in earlier reports, but the secret documents, shared by The New York Times, The Guardian and ProPublica, offer far more details of their ambitions for smartphones and the apps that run on them. The efforts were part of an initiative called the mobile surge, according to a 2011 British document, an analogy to the troop surges in Iraq and Afghanistan. An N.S.A. analyst s enthusiasm was evident in the breathless title   Golden Nugget!   given to a slide for a top-secret talk in 2010 that described iPhones and Android phones as rich resources, another document noted.

The scale and the specifics of the data haul are not clear. The documents show that the N.S.A. and the British agency routinely obtain information from certain apps, particularly those introduced earliest to cellphones.

With some newer apps, including Angry Birds, the agencies have a similar ability, the documents show, but they do not make explicit whether the spies have put that into practice. Some personal data, developed in profiles by advertising companies, could be particularly sensitive: A secret British intelligence document from 2012 said that spies can scrub smartphone apps to collect details like a user s political alignment and sexual orientation.

President Obama announced new restrictions this month to better protect the privacy of ordinary Americans and foreigners from government surveillance, including limits on how the N.S.A. can view the metadata of Americans phone calls the routing information, time stamps and other data associated with calls. But he did not address the information that the intelligence agencies get from leaky apps and other smartphone functions.

And while Mr. Obama expressed concern about advertising companies that collect information on people to send tailored ads to their mobile phones, he offered no hint that American spies have routinely seized that data. Nothing in the secret reports indicates that the companies cooperated with the spy agencies to share the information; the topic is not addressed.

The agencies have long been intercepting earlier generations of cellphone traffic like text messages and metadata from nearly every segment of the mobile network and, more recently, computer traffic running on Internet pipelines. Because those same networks carry the rush of data from leaky apps, the agencies have a ready-made way to collect and store this new resource. The documents do not address how many users might be affected, whether they include Americans or how often, with so much information collected automatically, analysts would see personal data.

 N.S.A. does not profile everyday Americans as it carries out its foreign intelligence mission, the agency wrote in response to questions about the program. Because some data of U.S. persons may at times be incidentally collected in N.S.A. s lawful foreign intelligence mission, privacy protections for U.S. persons exist across the entire process. Similar protections, the agency said, are in place for innocent foreign citizens.

The British spy agency declined to comment on any specific program, but said all its activities complied with British law.

Two top-secret flow charts produced by the British agency in 2012 showed incoming streams of information skimmed from smartphone traffic by the Americans and the British. The streams were divided into traditional telephony metadata and others marked social apps, geo apps, http linking, webmail, MMS and traffic associated with mobile ads, among others. (MMS refers to the mobile system for sending pictures and other multimedia, and http is the protocol for linking to websites.)

In charts showing how information flows from smartphones into the agency s computers, analysts included questions to be answered by the data, like Where was my target when they did this? and Where is my target going?

As the program accelerated, the N.S.A. nearly quadrupled its budget in a single year, to $767 million in 2007 from $204 million, according to a top-secret analysis written by Canadian intelligence around the same time.

Even sophisticated users are often unaware of how smartphones offer spies

a unique opportunity for one-stop shopping for information. By having these devices in our pockets and using them more and more, said Philippe Langlois, who has studied the vulnerabilities of mobile phone networks and is the founder of the Paris-based company Priority One Security, you re somehow becoming a sensor for the world intelligence community.

Smartphones almost seem to make things too easy. Functioning as phones to make calls and send texts and as computers to surf the web and send emails, they both generate and rely on data. One secret report showed that just by updating Android software, a user sent more than 500 lines of data about the phone s history and use onto the network.

Such information helps mobile advertising companies, for example, create detailed profiles of people based on how they use their mobile device, where they travel, what apps and websites they open, and other factors. Advertising firms might triangulate web shopping data and browsing history to guess whether someone is wealthy or has children.

The N.S.A. and the British agency busily scoop up this data, mining it for new information and comparing it with their lists of intelligence targets.

One secret British document from 2010 suggested that the agencies collected such a huge volume of cookies   the digital traces left on a mobile device or a computer when a target visits a website   that classified computers were having trouble storing it all.

 They are gathered in bulk, and are currently our single largest type of events, the document said.

This document from May 2010, redacted in places, is one of several undisclosed classified documents provided by Edward J. Snowden, the former N.S.A contractor, and shared by The New York Times, The Guardian and ProPublica.

The two agencies displayed a particular interest in Google Maps, which is accurate to within a few yards or better in some locations. Intelligence agencies collected so much data from the app that you ll be able to clone Google s database of global searches for directions, according to a top-secret N.S.A. report from 2007.

 It effectively means that anyone using Google Maps on a smartphone is working in support of a GCHQ system, a secret 2008 report by the British agency said.

(In December, The Washington Post, citing the Snowden documents, reported that the N.S.A. was using metadata to track cellphone locations outside the United States and was using ad cookies to connect Internet addresses with physical locations.)

In another example, a secret 20-page British report dated 2012 included the computer code needed for plucking the profiles generated when Android users play Angry Birds. The app was created by Rovio Entertainment, of Finland, and has been downloaded more than a billion times, the company has said.

Rovio drew public criticism in 2012 when researchers claimed that the app was tracking users locations and gathering other data and passing it to mobile ad companies. In a statement on its website, Rovio says that it may collect its users personal data, but that it abides by some restrictions. For example, the statement says, Rovio does not knowingly

collect personal information from children under 13 years of age.

The secret report noted that the profiles vary depending on which of the
ad companies   which include Burstly and Google s ad services, two of the
largest online advertising businesses   compiles them. Most profiles
contain a string of characters that identifies the phone, along with
basic data on the user like age, sex and location. One profile notes
whether the user is currently listening to music or making a call, and
another has an entry for household income.

Google declined to comment for this article, and Burstly did not respond
to multiple requests for comment. Saara Bergstrom, a Rovio spokeswoman,
said the company had no knowledge of the intelligence programs. Nor do
we have any involvement with the organizations you mentioned, Ms.
Bergstrom said, referring to the N.S.A. and the British spy agency.

Another ad company creates far more intrusive profiles that the agencies
can retrieve, the report said. The names of the apps that generate those
profiles were not given, but the company was identified as Millennial
Media, which has its headquarters in Baltimore.

In securities filings, Millennial documented how it began working with
Rovio in 2011 to embed ad services in Angry Birds apps running on
iPhones, Android phones and other devices.

According to the report, the profiles created by Millennial contain much
of the same information as others, but several categories that are listed
as optional, including ethnicity, marital status and sexual
orientation, suggest that much wider sweeps of personal data may take
place.

Possible categories for marital status, the secret report said, include
single, married, divorced, engaged and swinger ; those for sexual
orientation are straight, gay, bisexual and not sure. It is unclear
whether the not sure category exists because so many phone apps are
used by children, or because insufficient data may be available.

There is no explanation of precisely how the ad company defined the
categories, whether users volunteered the information or whether the
company inferred it by other means. Nor is there any discussion of why
all that information would be useful for marketing   or intelligence.

The agencies have had occasional success, at least by their own
reckoning, when they start with something closer to a traditional
investigative tip or lead. The spies say that tracking smartphone traffic
helped break up a bomb plot by Al Qaeda in Germany in 2007, and the
N.S.A. boasted that to crack the plot, it wove together mobile data with
emails, logins and web traffic. Similarly, mining smartphone data helped
lead to the arrests of members of a drug cartel hit squad in the killing
of an American Consulate employee in Mexico in 2010.

But the data, whose volume is soaring as mobile devices have begun to
dominate the technological landscape, is a crushing amount of information
for the spies to sift through. As smartphone data builds up in N.S.A. and
British databases, the agencies sometimes seem a bit at a loss on what to
do with it all, the documents show. A few isolated experiments provide
hints as to how unwieldy the data can be.

In 2009, the American and British spy agencies each undertook a
brute-force analysis of a tiny sliver of their cellphone databases.

Crunching just one month of N.S.A. cellphone data, a secret report said, required 120 computers and turned up 8,615,650 actors   apparently callers of interest. A similar run using three months of British data came up with 24,760,289 actors.

 Not necessarily straightforward, the report said of the analysis.

The agencies extensive computer operations had trouble sorting through the slice of data. Analysts were dealing with immaturity, the report said, encountering computer memory and processing problems. The report made no mention of anything suspicious in the data.

Hackers Transform Angry Birds Website Into 'Spying Birds' Following NSA Claims

The official Angry Birds website was defaced by hackers following reports that U.S. and U.K. intelligence agencies have been collecting user information from the game and other popular mobile apps.

Some users trying to access the www.angrybirds.com website late Tuesday were greeted by an image depicting the Angry Birds game characters accompanied by the text Spying Birds. The U.S. National Security Agency s logo was also visible in the image.

The NSA and Britain s Government Communications Headquarters (GCHQ) have been working together to collect geolocation data, address books, buddy lists, telephone logs and other pieces of information from leaky mobile apps, The New York Times reported Monday based on documents provided by former NSA contractor Edward Snowden.

Mobile apps commonly collect data about their users and share it with advertising networks, which then use the information to build user profiles for targeted advertising.

A secret 20-page GCHQ report from 2012 contained code needed to extract the profiles generated when Android users play Angry Birds, The New York Times reported. It s not clear if and how this data collection happens, but the reports were apparently enough to anger some hackers.

The defacement of the Angry Birds website seems to have been the result of a DNS (Domain Name System) attack where the site s name servers were swapped with others under the attackers control.

  The defacement was caught in minutes and corrected immediately, said Saara Bergström, vice president of marketing communications at Rovio Entertainment, the Finnish company that develops Angry Birds. The end user data was in no risk at any point.

Bergström said the attack was similar to the one against The New York Times last year, referring to an incident where attackers pointed the nytimes.com domain to a server they controlled by changing its DNS settings.

""Rovio does not allow any third party network to use or hand over personal end-user data from Rovio s apps.""

Because of how DNS changes propagate on the Internet, the incident was only visible to some users.

In many areas the attack was not visible at all, but in some affected
areas it might take time for the correct information to be updated,
Bergström said.

This delay is caused by how DNS resolvers servers that resolve domain
names to IP (Internet Protocol) addresses cache records. Some servers
might cache the information for a particular domain for a longer time than
others, in which case changes won t be visible to users that rely on those
servers until the cached record expires.

A copy of the angrybirds.com defacement can be viewed on Zone-H, a website
defacement archive. It is attributed to a hacker using the handle Anti-NSA.
Angry ads?

Rovio issued a statement Tuesday on its website denying that it
collaborates or shares data with any government spy agencies.

 The alleged surveillance may be conducted through third party
advertising networks used by millions of commercial websites and mobile
applications across all industries, the company said. If advertising
networks are indeed targeted, it would appear that no internet-enabled
device that visits ad-enabled websites or uses ad-enabled applications
is immune to such surveillance. Rovio does not allow any third party
network to use or hand over personal end-user data from Rovio s apps.

Yahoo Mail Hacked: What To Do If You ve Been Affected

Yahoo Mail users, we have some bad news: It s time to change your e-mail
password.

In a company blog post Thursday night, Yahoo revealed that a number of
users passwords and usernames were exposed to cyber-attackers who used
malicious computer software to gain access to lists of Yahoo Mail
credentials.

The information was likely collected from a third-party database, Jay
Rossiter, Yahoo s senior vice president of platforms and personalization
products, wrote in the posting.

The company is resetting passwords on accounts that have been affected and
is taking steps to allow users to re-secure their accounts. It is sending
notification e-mails instructing those users to change their passwords;
users may also receive a text message, if they ve shared their phone
number with the company.

It s a song-and-dance that users may be tiring of, but it is important for
Yahoo account holders who were swept up in the attack to change their
passwords for immediately. They should also change their log-in
credentials for any account that may share their Yahoo password,
particularly if they use their Yahoo e-mail as their username. The same
is true if you use a similar e-mail address as the username   it s not a
big leap for hackers to think that you may be both jdoe@yahoo.com and
jdoe@gmail.com.

Finally, everyone should also be on the lookout for spam, as the attack
also appears to have picked up names and e-mail addresses for the most

recent contacts from affected accounts, according to the company s post.

If you get an odd e-mail from the Yahoo account of someone you know, ignore the message, and do not click on any links in the message. (It s also be nice to let the person whose account has been hacked know about the fraudulent messages, so they can warn others to avoid the e-mails.)

Yahoo has apologized for the inconvenience and has said that it has taken additional measures to block attacks on its system. The company did not immediately respond to a request asking how many of its users were affected.

Yahoo is the world's second-largest e-mail provider, and has an estimated 273 million users, according to a report from the Associated Press.

Victim of Epic Hack Points Finger at GoDaddy and PayPal

Passwords, even strong ones, aren't enough to protect you. Your online accounts are only as safe as the security policies of the companies that hold them.

At least that's the apparent lesson to be learned from Naoki Hiroshima's epic account of how one hacker used a series of simple social-engineering tactics to gain control of his online accounts without using a single password.

Naoki Hiroshima claims to have tweeted using the @N handle since signing up for Twitter in 2007. In that time, he said, he has fended off multiple attempts by attackers to take control of the coveted one-character account. He claims he was once even offered $50,000 in exchange for the handle.

These attempts were unsuccessful   until Jan. 20.

On that day, according to Hiroshima's account, a hacker posing as a PayPal employee called PayPal's customer service and was ultimately able to obtain the last four digits of Hiroshima's credit card.

The hacker then called GoDaddy's customer service and, after providing the numbers obtained from Paypal, was allowed to "guess" the first two digits of the credit card on file. After providing this information, the hacker gained access to Hiroshima's account and promptly changed the account information, effectively locking the real Hiroshima out of the account.

For Hiroshima, who used GoDaddy to host the domains for his personal websites and email, the significance of being shut out of this account was huge:

    Most websites use email as a method of verification. If your email account is compromised, an attacker can easily reset your password on many other websites. By taking control of my domain name at GoDaddy, my attacker was able to control my email.

Once in control of Hiroshima's email, the hacker also took control of his Facebook account.

Around this time, Hiroshima says he realized his Twitter account was the target of the attack. He changed the email linked to the account, preventing his attacker from changing the password.

Undeterred, the hacker contacted Hiroshima with an ultimatum: Turn over @N, or lose all of his GoDaddy domains forever. Hiroshima, who had so far been unsuccessful in his attempts to regain control of the account, relented.

True to his word, the hacker returned the GoDaddy account to Hiroshima, now tweeting from @N_is_stolen, and revealed the the details of how he carried out the attack.

If this story sounds familiar, it's because it bears striking similarities to the the 2012 hacking of Wired reporter Mat Honan, who had his iPad, iPhone and MacBook wiped when a hacker used similar social-engineering methods to obtain Honan's iCloud password. Like Hiroshima, the ultimate target of that attack was Honan's Twitter account. Honan nearly irrevocably lost much of his person photos and media, and Hiroshima didn't want the same thing to happen to him.

"I remembered what had happened to @mat and concluded that giving up the [Twitter] account right away would be the only way to avoid an irreversible disaster," Hiroshima wrote.

Honan had his accounts restored and even managed to eventually restore much of the data from his wiped Macbook.

It's not yet clear whether Hiroshima will be as lucky, though it appears the sudden publicity his account has drawn may have given GoDaddy, who did not respond to Mashable's request to comment, more incentive to help him.

In a statement to Mashable, Twitter said the company does not comment on specific accounts but confirmed they are investigating the report.

On its part, PayPal has denied disclosing any credit card information to Hiroshima's attacker.

"Our investigation confirmed PayPal did NOT disclose any credit card details," the company said in a tweet Wednesday.

PayPal later revealed more details about their internal investigation in a blog post Wednesday. The company called Hiroshima's situation "difficult" but reiterated they did not disclose any of his account information and said his account was never actually compromised.

We have carefully reviewed our records and can confirm that there was a failed attempt made to gain this customer s information by contacting PayPal.

PayPal did not divulge any credit card details related to this account.

PayPal did not divulge any personal or financial information related to this account.

This individual's PayPal account was not compromised.

A New Service Will Let You Borrow Your Neighbor's Wi-Fi for a Stronger Connection

We ve all been there: Your Wi-Fi goes out and, as you wait on hold with your provider s customer service rep, your mouse hovers over your neighbor s networks. If only you could just hop on TheNewmanFamily Wi-Fi, you would have sweet, sweet Internet again. Besides, they re probably not even home!

Spanish broadband provider Telefónica has been experimenting with a system to put that temptation to use, as detailed in an article from Wired UK. Their solution, named BeWifi, gathers bandwidth from Wi-Fi routers in a local area, and uses that to strengthen the speed of the Internet connection for whomever is actively online at that time.

How does it work? Since 2008, Telefónica has been developing over-the-air software that aggregates the signals of a community s routers. It blends the bandwidth from every router to supplement their usual Wi-Fi connection at home. According to Telefónica s Director of Product Innovation and Research Pablo Rodriguez, you ll always get at least the bandwidth you paid for (a big promise in itself for anyone who s ever used Time Warner).

"Your broadband connection is not used 100 percent of the time," Rodriguez told Wired U.K.. If you bring [connections] together smartly and manage to aggregate the spare capacity   [it s] a much better customer experience.

BeWifi is still in testing stages (and only in Spain), and results so far have demonstrated some limitations to the service. First of all, the software only works effectively in densely populated areas like cities. Second, the company has yet to roll out plug-and-play routers that don t require installation from their company s engineers. But the service s pilot program, according to Rodriguez, was successful in doubling some customers s connection speed. He also mentioned that one user was experiencing an outage, but didn t even know it, because his connection was supported by the community network.

Though there is still clearly a lot to iron out here, it s exciting to see technology that could potentially make Internet connection in urban settings less horrible all through some old-fashioned neighborly cooperation, no less.

Will shared Wi-Fi ever make it to America? Most Internet Service Providers expressly prohibit sharing your Wi-Fi with multiple households, though there are signs that might be easing. We ve already seen whisperings of this approach from U.S. providers like Comcast, which launched a Neighborhood Hotspot initiative this summer for its Xfinity Internet customers. Even non-subscribers are able use the separate hotspots for free twice per month for up to an hour each time. Though Comcast s strategy is a little less advanced than what Telefónica has experimented with, it s nice to see that companies aren t just banking on more expensive technologies and Google Fiber for the future.

Take a Trip Down Facebook s Privacy Back Roads
To Keep Your Posts Away from Prying Eyes

I was goofing around on Facebook the other day when I stumbled into a section I d never seen before, called the Activity Log. It s accessible via a clearly labeled link at the top of your profile page. This seemingly endless scrolling list contained not only every post I d ever made, but also all my likes, comments and even mentions of me by other Facebook users.

Essentially, it was a kind of cute if occasionally embarrassing tally of the goofy pictures and musings I ve posted of my kids, my meals and my travels.

Once I found the list, I was more than a little curious to check my privacy settings. The occasional public post may be a little embarrassing or even harmless. Generally speaking, though, it s not a good idea to make all your private activity public. Hackers, identity thieves and even, in some cases, real thieves, can use the info to crack your online accounts or break into your house when you re not there. And Facebook has changed its privacy setting options and policies more than a few times, making it doubly important to review your activity.

And in that regard, the Activity Log turned out to be highly informative. Along the top-right side of each individual listing was a tiny icon. Most were Facebook s familiar friends icons, but some were a gear icon, and a few had a globe icon.

Investigating further, I discovered that each icon disclosed the privacy settings of the particular item posted. Hovering my mouse pointer over the friends icon revealed just whose friends could see the item   usually mine or those of whomever had posted about me. The gear icon indicated that someone had created a limited, custom group to see the item   just people from work, say, or everyone except people from work.

But it was the globe icon that was ultimately the most intriguing. It signified a public post. And many of the public posts seemed to be by friends who don t usually disclose everything on Facebook publicly.

After reaching out to some of these posters, most were puzzled   it seems they d posted publicly by accident. That used to happen pretty easily with Facebook s mobile apps, although the company has made improvements, especially on iOS, to minimize the problem.

Your own overshared posts can be rectified right from the Activity Log. Hover your mouse near the globe icon and click on the blue triangle that appears. A menu drops down with various privacy settings, including Only Me, Friends and Public. Click your preference, and the problem is solved.

However, only the person who posted the item can change the setting. That can be a bit annoying if you ve made a flippant or impolitic comment on someone else s post or photograph without realizing that your friend had left the item and its following chain of comments public for the world to see. In that situation, you have to ask your friend to change the setting, or, worst case, delete your comment.

There was one additional puzzling aspect to my Activity Log. It seems at some point, way back, I agreed to let Spotify, the online music service, post to my Facebook timeline. I don t really listen to much on Spotify anymore, though. It s my teenage son who uses it most.

So, there on my timeline, apparently going back years, was a catalog of cool, hip songs that my friends probably thought I was sampling. These posts never showed up on my own timeline as I saw it   just when friends looked at my timeline from their point of view.

In this case, the accidental posting by the Spotify app was pretty innocuous. It may even have enhanced my reputation as some sort of pop music guru, thanks to my son s eclectic and savvy selections. But you can imagine that there might be apps you wouldn t want making these kind of semi-invisible posts.

To fix the problem, go to Facebook s Settings page and click on Apps. You might be surprised to see just how long a list of apps you ve given permission to at least access your Facebook account. On the right side of each app s listing is an Edit link. Click it, and you can see just what the app s been up to and what permissions it has to post. From here, you can revoke the permissions or delete the app s access to your account completely.

Besides reviewing the Activity Log for public items, a potentially lengthy process if you ve been active on the social network for a few years, Facebook also provides a way to make wholesale changes to all your own posts.

Go to Facebook s privacy settings page and look at the who can see my stuff section. There s a subsection called Limit the audience for posts you ve shared with friends of friends or Public. Clicking the link takes you to a tool for changing the privacy settings for all older posts.

Again, people s privacy tolerance differs, and yours may evolve over time. But if you re worried about what you ve said and done on Facebook, be sure to take a look at your Activity Log. It s the key to privacy peace of mind, Facebook-wise at least.

FCC Begins Voluntary TDM-to-IP Transition Experiments,
Measuring Consumer Impact

The FCC is getting ready to conduct IP service transition tests, a move that was lauded by U.S. incumbent telco AT&T, which says that current regulations don't apply to the emerging IP-based wireline network environment.

The new order considers a broad set of voluntary experiments to test what impact the migration from TDM to IP-based technology will have on various sets of end-users.

"Driven by developments in the marketplace, technology transitions in communications networks are already well underway," the FCC said in its order. "They include, for example, the transition from plain old telephone service delivered over copper lines to feature-rich voice service using Internet Protocols, delivered over coaxial cable, fiber, or wireless networks."

Through these experiments, the FCC said it will gather information in three broad areas: service-based experiments; targeted experiments and cooperative research; and data improvement.

Incumbent telcos such as AT&T and Verizon (NYSE: VZ) still have to abide by the Carrier of Last Resort (COLR) rule from 1913 that says that every American household should have access to a phone line.

However, both telcos have continued to see their traditional POTS revenues and overall subscriber bases decline as customers replace their landline phones with wireless or a VoIP line. AT&T's consumer POTS access lines declined from 15.7 million to 12.4 million lines between 2012 and 2013. Likewise, Verizon reported that voice lines declined to 11.3 million in Q4 2013.

In a blog post, Jim Cicconi, AT&T's senior executive vice president-External and Legislative Affairs, praised the FCC's move.

"Beginning the process for achieving this transformation is overdue, and all of us should recognize the sense of urgency Chairman Wheeler and his team have brought to this issue," wrote Cicconi. "They quickly recognized and credited the leadership shown many months earlier by Commissioners Rosenworcel, Pai, and Clyburn, as well as the clear public support of Commissioner O'Rielly, to build a unanimous vote for moving forward. This is visionary both for its break with the past, its recognition of the future, and its unanimity in a time of partisan strife."

Following a call last year by former FCC Chairman Julius Genachowski to conduct trials, Wheeler cited the TDM-to-IP migration as one of his initial priorities when he became the regulator's chairman in November. Calling it the Fourth Network Revolution, he proposed the regulator put out an order addressing the matter at its upcoming meeting in January.

Wheeler's quick call to action got the attention of AT&T, which has set 2020 as the year when it wants to transition off legacy TDM to all IP networks. It has asked the regulator for permission to conduct IP trials in two of its 4,500 wiring centers and had expressed frustration over what it called the regulator's lack of action.

Proposals from AT&T and other interested parties are due by Feb. 20 and will be followed by a public comment and reply period ending on March 31. The FCC will make the final decision on the proposals at its meeting in May.

Microsoft Needs a Sorcerer, Not the Server Guy

Hopefully, reports that Satya Nadella - Microsoft's cloud and enterprise chief will be Microsoft's next CEO, are just a lot of hype.

Nadella is brilliant. Since he's been top enterprise guy, Microsoft's business division's success is practically a mirror image of its consumer's. The company has adroitly moved its iconic on-premise business wares, including Office and Windows Server, to excellent, streamlined cloud platforms.

Office 365 and Azure are making great gains in adoption. Gartner and other industry analysts show Azure heartily gobbling into Amazon's cloud platform market share. Hyper-V keeps nipping at VMware's heels. While enteprises will take time to adopt Windows Server 2012 en masse, the new server OS (dubbed "Cloud OS" by Redmond) is bound to find a comfortable place in business datacenters as organizations upgrade their server

infrastructures.

Enterprise Microsoft is doing just fine. And Nadella is a big reason for that health. However, Nadella's success in the business side of Microsoft does not mean he can translate that into success on the consumer side. It's almost as if the powers that be (investors, board of directions, etc) who make these kind of decisions, took a look at the team currently making Microsoft the most profit and decided that team's head should be the new CEO.
Opinions

If so, that's the wrong approach. It's exactly that type of stagnant, business- and profit-oriented, 90s tycoon mindset that keeps Microsoft from missing its mark in the consumer space.

Redmond needs the opposite of what Apple needed when Steve Jobs passed. Apple was and remains rich in creativity and innovation (although some may argue that innovation has been slipping of late). It's almost as if Jobs's essence flowed into the engineers, designers, and other Apple employees and remains so even after his death. With Apple already abundant in creative energy, a bottom-line, business-savvy Tim Cook was a good choice for its new CEO.
Advertisement

Microsoft knows business. What it needs now is magic, a CEO strong in creativity. Someone who can shake out the stodginess and awaken some real innovation in the consumer side of the company. A new CEO who will know well enough to not micro-manage the already-thriving enterprise side of Microsoft and will give a good kick in the pants to the consumer side.

Personally, I would love to see what Julie Larson-Green, the executive vice president overseeing devices like the Xbox and Surface tablet, would do if freed from the direction of Steve Ballmer. I think she could really flourish at the top and take the consumer side to a new height.

Another great option would be just to recruit from outside of Microsoft. Bypass the Ballmer holdovers completely. Get an executive from the mobile or the gaming industry with a proven track record of steering the company in a creative direction that resulted in massive profit.

What Nadella and the teams that develop the enterprise portfolio at Redmond know best are the desires of the business community. Going with a CEO who uses business savvy to influence consumer offerings is directly counter to current tech trends. It's the consumer products and cloud services and start-ups that are disrupting and re-shaping business technology. Microsoft's new CEO should be driven more by creativity than profit.

Microsoft Finally Realizes That People Hate Windows 8's Live Tiles

It s official: Microsoft realizes that most desktop users have no use for the Live Tiles interface. The Verge reports that the next update of Windows 8.1 will make the platform boot up to desktop mode by default, which means that people who buy new Windows 8.1 PCs with the latest update won t have to look at Live Tiles when they first flip on their computers.

We understand that Microsoft has been paying close attention to telemetry

data that shows the majority of Windows 8 users still use a keyboard and mouse and desktop applications, The Verge writes. This same telemetry data was used to justify the removal of the Start button shortly before the Windows 8 release, and contributed to its eventual return in Windows 8.1. Microsoft may have wanted to push touch computing to the masses in Windows 8, but the reality is that users have voiced clear concerns over the interface on desktop PCs.

This takes us back to Apple CEO Tim Cook s joke about how trying to merge a desktop OS with a tablet OS was the equivalent of trying to merger a toaster and a refrigerator. While Microsoft s attempt to create one common interface for all its devices was certainly a noble experiment, it hasn t exactly been a successful one so far and the company seems to know it.

HP Brings Back Windows 7 'By Popular Demand'

HP really wants people to buy a Windows 7 PC instead of a Windows 8 machine. The PC maker has been emailing customers over the weekend noting that "Windows 7 is back." A new promotion, designed to entice people to select Windows 7 over Windows 8 with $150 of "savings," has launched on HP s website with a "back by popular demand" slogan. The move is clearly designed to position Windows 7 over Microsoft s touch-centric Windows 8 operating system.

In fact, if you browse to HP s home section and navigate to desktop PCs then you ll only be presented with Windows 7 machines by default as no Windows 8 PCs are listed until you start customizing the section using optional filters. The laptop section does include Windows 8 machines, but it also prominently advertises a Windows 7 laptop. Even HP s all-in-one section promotes the company s 21-inch Android-powered PC over Windows 8 alternatives.

HP s "back by popular demand" wording is a clear knock towards Windows 8 which has struggled with perception issues thanks to what some see as a confusing mix of desktop and tablet-style computing. Microsoft has tweaked some parts of the OS with Windows 8.1, but it looks like Windows 9 will bring more significant changes and a move away from the Windows 8 branding. In the mean time, HP is the first PC maker to take advantage of Windows 7 as a selling point over Windows 8, and it follows similar moves from OEMs who chose to promote Windows XP over Windows Vista years ago.

Expectant Parents Letting Internet Vote On Name Of Baby

In what s sure to be the first in a couple s long line of fabulous parenting decisions, two soon-to-be parents have asked the Internet for help naming their daughter.

With the approval of his (probably long suffering) wife, the husband set up namemydaughter.com, where users can vote for their favorite first and middle names for the unborn baby girl.

The husband explained himself and appealed to potential voters on Reddit, because obviously:

"I was sitting on the end of the bed after coming home from work and the idea hit me. I tend to be very forward person (this gets me in a lot of trouble lol) and I just blurted it out - Hunny, I am going to ask the internet what we should name our daughter!

She was supportive right from the start. I think at first she didn t think I was actually going to do it. But once the domain was registered she knew it was real.

Hell when I saw that namemydaughter.com was available I just knew that was the sign that I HAD to do it.

That s simply ridiculous reasoning. Runamarathon.com is probably available right now, but that doesn t mean I m suddenly not going to spend two hours watching The Bachelor tonight and stuffing my face with cheesy jalapeno Pop Chips.

Anyway, in news that should surprise no one, the crazies of Reddit are really getting into it. Though surprisingly normal name Amelia Mae is currently in first place, it s followed by Cthulu All-Spark. Names likes Charlotte, Leslie, Renee and Meagan also top the list, but so do Ixtley, Megatron, Slagathor, Titanium, and Salad. That, ladies and gentlemen, is what happens when you specifically solicit Reddit for help in your stupid baby naming plans.

Update: "Cthulhu All-Spark" has climbed into first place as of noon EST on Tuesday afternoon.

The husband established the rule that users can only vote for each name once per household per day, wisely protecting his daughter from the neckbeards who d inevitably spend hours voting for SwordOfDestiny SuperNova until their thumbs were too sore to play Warcraft that night.

But mayhaps this loony husband isn t fully insane. At the top of the site, he declares: Unfortunately internet I know better than to trust you. We will ultimately be making the final decision, Alas my daughter shall not be named WackyTaco692. Sorry guys the wife wouldn t go for a free for all.

The very lucky baby is due April 2, so if we start voting now, we can probably make BeyoncØ happen. Let s do it.

=~=~=~=

internet site, in whole or in part, by any agent or means, without
the expressed consent or permission from the Publisher or Editor of
Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do
not necessarily reflect those of the staff, or of the publishers. All
material herein is believed to be accurate at the time of publishing.